DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

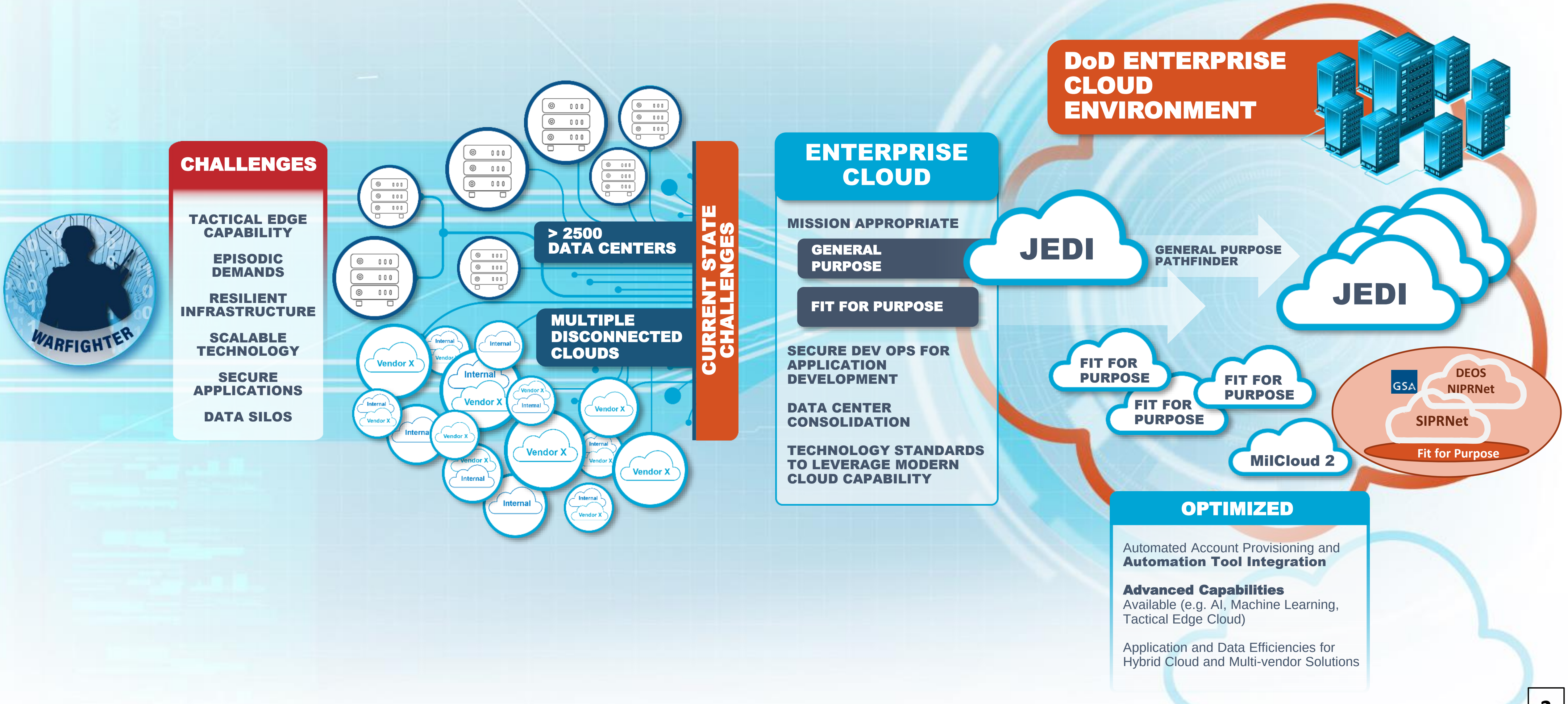
Defense Enterprise Office Solutions (DEOS) and Enterprise Collaboration and Productivity Services (ECAPS)

Karl Kurz
DISA Unified Capabilities Portfolio

Kevin Tate
DoD Chief Information Office

DoD ENTERPRISE CLOUD STRATEGY

Path to Multi-Vendor, Multi-Cloud Environment



CHALLENGES

TACTICAL EDGE CAPABILITY

EPISODIC DEMANDS

RESILIENT INFRASTRUCTURE

SCALABLE TECHNOLOGY

SECURE APPLICATIONS

DATA SILOS

> 2500 DATA CENTERS

MULTIPLE DISCONNECTED CLOUDS

CURRENT STATE CHALLENGES

ENTERPRISE CLOUD

MISSION APPROPRIATE

- GENERAL PURPOSE
- FIT FOR PURPOSE

SECURE DEV OPS FOR APPLICATION DEVELOPMENT

DATA CENTER CONSOLIDATION

TECHNOLOGY STANDARDS TO LEVERAGE MODERN CLOUD CAPABILITY

DoD ENTERPRISE CLOUD ENVIRONMENT

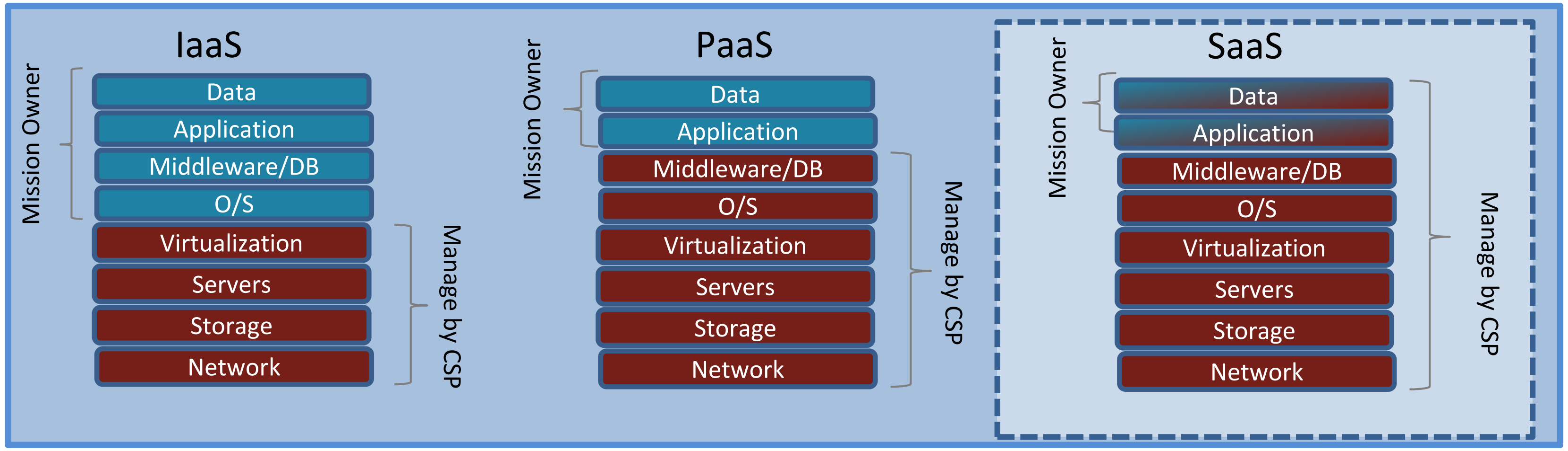
OPTIMIZED

Automated Account Provisioning and **Automation Tool Integration**

Advanced Capabilities Available (e.g. AI, Machine Learning, Tactical Edge Cloud)

Application and Data Efficiencies for Hybrid Cloud and Multi-vendor Solutions

Cloud Service Model for ECAPS



SaaS Benefits

- Single ecosystem that facilitates greater interoperability and seamless integration
- Increased COOP/redundancy across Department
- Rapid security updates at server level
- Innovation at the pace of industry
- Increased records management and legal hold capability at no additional cost
- Greater visibility into costs/expenditures

Enterprise Collaboration and Productivity Services

What is ECAPS? **Outsourced DoD Enterprise Commercial Cloud Service Solutions that facilitate communications, collaboration and productivity across all organizational levels to improve the conduct of day-to-day business and missions**

Why is ECAPS Important? **Current federated, segmented and competing approaches result in:**

- **Increased software & infrastructure costs**
- **Lack of integration across Department**
- **Increased security risks**
- **Current Industry Model is End of Life or Current Approach not aligned to industry direction**

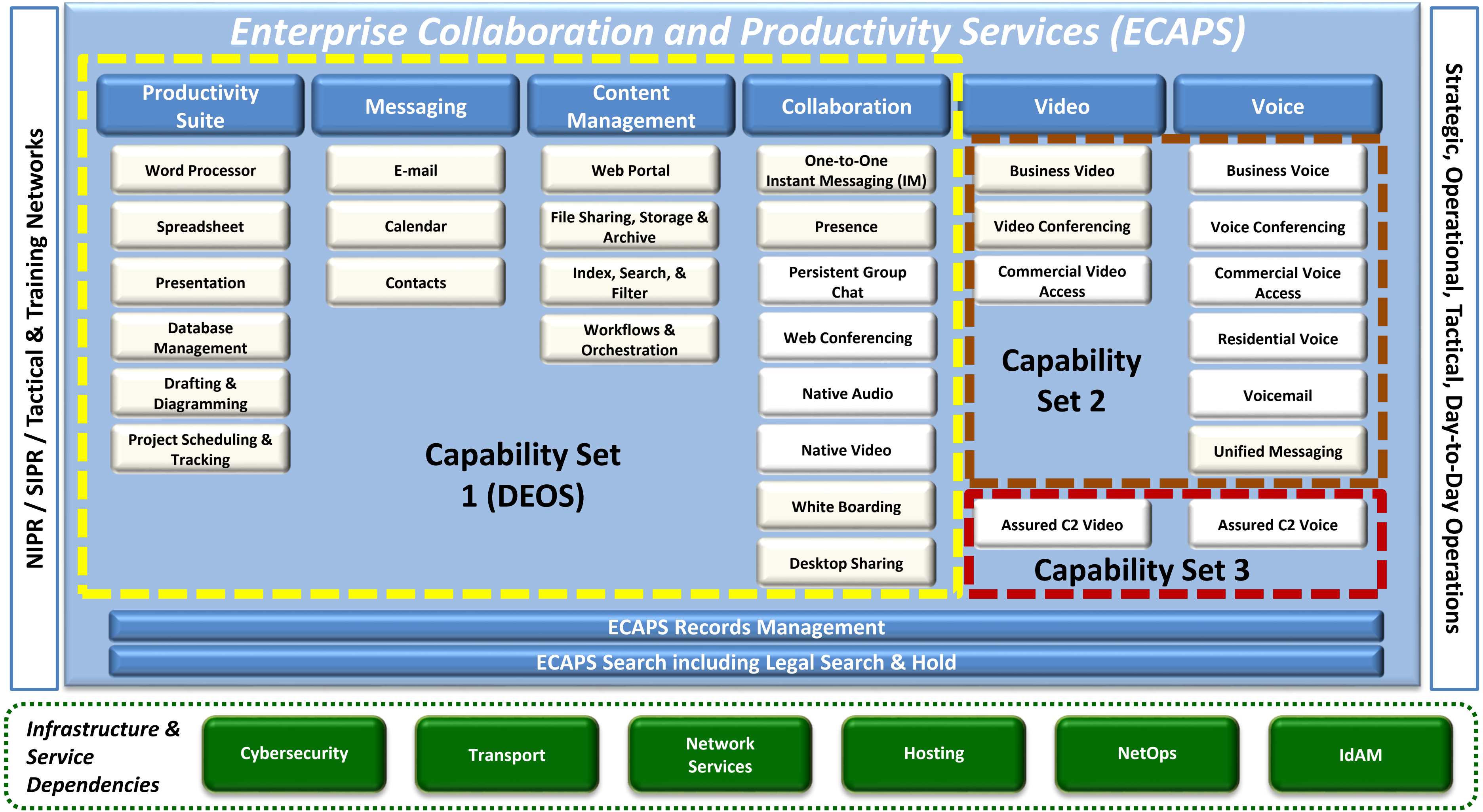
> **“To achieve greater Departmental efficiency and savings, we must now pursue cross-enterprise consolidation of business activities… I direct you to further this work by exploring efficiencies across the following core business functions:…cyber and information technology management.” (Secretary of Defense Mattis - February 17, 2017)**

ECAPS Strategic Goals

GOALS:	Description:
Goal 1: Advance and evolve the DoD enterprise to support effective productivity across all mission sets	Improves the collaboration, productivity, and communication capabilities to support the secure sharing of information, infrastructure, and knowledge
Goal 2: Implement a standardized set of capabilities that allows for ubiquitous access and freedom of movement within and across all DoD enterprise organizations and security boundaries	Enables authorized users to access capabilities and services anywhere and anytime
Goal 3: Provide dynamic information access	Establishes policies and standards that give the ability to share the right information with the right people at the right time, regardless of location
Goal 4: Guide consistent, continuous, and efficient acquisition, and implement agile capability insertion	Creates a framework and standards for rapid evaluation and adoption of emerging capabilities

ECAPS Vision and Scope

Vision - integrated information sharing capabilities that allow for a near real-time seamless communication and collaboration and provide freedom of movement across the DoD Enterprise.



NIPR / SIPR / Tactical & Training Networks

Enterprise Collaboration and Productivity Services (ECAPS)

Productivity Suite	Messaging	Content Management	Collaboration	Video	Voice
Word Processor	E-mail	Web Portal	One-to-One Instant Messaging (IM)	Business Video	Business Voice
Spreadsheet	Calendar	File Sharing, Storage & Archive	Presence	Video Conferencing	Voice Conferencing
Presentation	Contacts	Index, Search, & Filter	Persistent Group Chat	Commercial Video Access	Commercial Voice Access
Database Management		Workflows & Orchestration	Web Conferencing		Residential Voice
Drafting & Diagramming			Native Audio		Voicemail
Project Scheduling & Tracking			Native Video		Unified Messaging
			White Boarding	Assured C2 Video	Assured C2 Voice
			Desktop Sharing		

Capability Set 1 (DEOS)

Capability Set 2

Capability Set 3

ECAPS Records Management

ECAPS Search including Legal Search & Hold

Strategic, Operational, Tactical, Day-to-Day Operations

Infrastructure & Service Dependencies

Cybersecurity | Transport | Network Services | Hosting | NetOps | IdAM

Defense Enterprise Office Solutions (DEOS)

DoD-wide *single* enterprise solution for common communication, collaboration and productivity. DEOS will be mission effective, secure, cost-effective, efficient, ubiquitously accessible, intuitive and enable DoD to operate and fight worldwide.

- **Department-wide need to offer greater functionality and efficiency**
- **Support tactical-edge environments**
- **Create a simpler, defensible perimeter by reducing DoD's IT Footprint**
- **Streamline information access and data sharing across the DoD**
- **Strengthen DoD Cybersecurity Posture & Leverage Joint Collaboration Capabilities**
- **Leverage proven commercial capabilities**

DEOS Next Steps

- DoD has partnered with GSA to issue a DoD-wide GSA Schedule 70 Blanket Purchase Agreement (BPA) for DEOS:
  - GSA leads contracting activities
  - DEOS PMO with DoD Services leads technical evaluations leading to BPA award
  - DEOS PMO leads stand up, technical integration, testing, and configuration management
  - Services will work directly with GSA to issue Task Orders for migration of their services to DEOS
  - DISA PMO will gather Department-wide lessons learned and assist Services and Agencies in migration prep and migration activities

- Significant Milestones:
  - Spring 2019: GSA releases Final RFQ
  - Summer 2019: GSA awards Blanket Purchase Agreement and initial task order to single prime contractor
  - Fall 2019: Integration testing and initial operational testing
  - FY20-22: DoD migration to DEOS

Migration Prep Checklist

DEOS
Defense Enterprise Office Solutions

The following items were derived from modeling and simulation analysis performed by the DEOS Program Management Office (PMO) to identify potential challenges with adopting and implementing a enterprise commercial cloud service. Certain items outlined below may not be applicable to local base/post/camp/stations.

General Planning/Change Management

1.	Notify your users about the change	Communicate the upcoming change and let users know at a high level the plan and how it will impact them.
2.	Identify IT Support Staff with whom the DEOS Migration Team (MT) will coordinate.	Identify POCs with knowledge of and access to Active Directory, Microsoft Exchange, network, and security infrastructure.
3.	Determine the DEOS services your organization will utilize	DEOS will contain email, office productivity, organizational content storage, personal storage, native audio, native video, and web conferencing.
4.	Analyze your user base and determine what type of client experience is required	Define whether your organization will utilize the DEOS thick client(s), browser based access only, or both as there is potential for cost savings if a thick client suite is not required.
5.	Plan and prepare for user and data migration	Identify the initial set of users to migrate as well as locations. Evaluate bandwidth at all locations and determine if sufficient for migration and ongoing service. Evaluate organizational data and determine what should be migrated to include SharePoint and local drives. Reduce unneeded data to optimize the migration.

About DEOS ...

DEOS will be a commercial cloud-based enterprise service that will provide office communication and collaboration tools for DoD personnel. This service will support Continental U.S. (CONUS) and outside continental U.S. (OCONUS) locations on the NIPRNet, SIPRNet, and Denied, Disconnected, Intermittent, and Limited Connectivity (D-DIL) environments regardless of compute platforms.

Base/Post/Camp/Station Preparation

6.	Evaluate current links to DISN and order upgrades/new links according to projected needs	Bases with under a 1GB link may experience performance issues @ 1,500 simultaneous users; Begin link bandwidth analysis at least 120 days prior to migration start.
7.	Review desktop configurations and ensure in alignment with DoD CIO Oct 2015 Windows 10 Memorandum	Upgrade to Windows 10 is recommended prior to migration depending on the services (e.g. email, conferencing, etc.) that will be consumed.
8.	Identify all firewalls and access rules in path to the DISN	Evaluate entire path from user enclaves to DISN network to identify owners/POCs for coordination.
9.	Collect enterprise network settings (DNS, Proxies, DHCP, NTP, etc)	Local settings may conflict with enterprise settings once you transition, so local network administrators may need alter them during migration.
10.	Identify all mobile users within your organization including Blackberry, IOS, & Android users	Are you using DMUC or DMCC? If providing local mobility services, devices may need to be updated to work with the new service? Are you working towards soft certificate updates via PureBred to ensure delivery of email to mobile devices.
11.	Plan/schedule training for Help Desk and Support teams	Once awarded, DEOS administrator training will be required for partner deployment of DEOS clients and reconfiguration of user desktop applications.
12.	Identify/document current details for all Email users	Include desktop client and Webmail users, and both NIPR & SIPR users. Be sure to include all systems (e.g. a user may have a DEE and local Service account).
13.	Identify/document current details for all Non-person entity (NPE) mailboxes, including type, descriptions, and owners	Include both distribution lists and mailbox enabled security groups. Identify/document NPEs utilizing soft certificates regenerated for submission to DISA and inclusion in GAL.
14.	Begin planning for reducing mailbox sizes, cleanup folders, archiving to pst files, and prepare for migration.	It is recommended that communications on user migration activities begin at least 60 Days prior to migration, and include repeated notification to users to reduce unneeded emails and personal file storage.
15.	Inventory all Email client software versions	Be prepared to update existing client software, if needed. Include all desktop & mobile users.
16.	Identify external application dependencies on DEE or other mail systems for calendaring or conference room free/busy information	Local Jabber or Skype client may pull from your local outlook client or from DEE APIs to pull in calendar information. A migration plan/feasibility study from the current systems to DEOS will need to be conducted.
17.	Review current records management requirements and solutions	Determine your group's RM requirements. Identify users with Capstone requirements (e.g. full automated NARA compliance) and determine if will need to migrate current Capstone user data to the cloud or if it will need to remain in place. Collect details on any applications (Symantec Enterprise Vault, CommVault) that integrate with or connect to existing Email service for archiving or storage.

CAC/Certificate Preparation

18.	Update user profile contact information in milConnect	Click to access DMDC instructions on updating a user profile on milConnect.
19.	Update personal profiles in milConnect to activate PIV certificates in compliance with FIPS 201	PIV will be the primary certificate on the DEOS platform for authentication. Go to https://www.dmdc.osd.mil/self_service to activate PIV. (Note - Java Runtime Environment (JRE) must be enabled on the browser).

Mission Partner/Special Access

20.	Review requirement for Foreign National or Mission Partner Accounts	Inventory existing special or non-standard accounts and evaluate if still needed. Identify their login method if non-standard and evaluate.

Content Management

21.	Collect details on all SharePoint or other document sharing sites (DEPS etc.), including users, ownership, total size, directory structure, and any customizations	Review current site and site content and determine if it is still relevant and accurate. Don't migrate content that is not needed. Use this as an opportunity to prune your data and to determine who will need to access it going forward.
22.	Third party products or heavily customized functionality or workflows	Inventory any 3rd party products implemented. Determine if really need or if may be able to streamline and go with SaaS built-in capabilities to reduce cost and complexity.

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**

visit us

DISA
Booth 1929

follow us

Facebook/USDISA

Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at **www.disa.mil/about/industry-partners**.